Amendments to the Specification

On page 4, lines 1-22, please replace the existing paragraph with the following substitute paragraph:

Prior to commencing a data exchange session between an implanted IMD and an external source capable of long range telemetry, such as provided by an RF programmer, repeater or wireless computing device, patient/clinician authentication must be completed, during which a crypto key is identified and retrieved for use during the data exchange session. The crypto key is maintained on a secure key repository and can be used to authenticate individual commands, check data integrity, and, optionally, encrypt sensitive information, including any [[PHI,,]] PHI, or a combination of the foregoing, when transmitted over a long range telemetric link. The crypto key can be either pre-programmed and persistently stored on the IMD, or can be dynamically generated on the IMD, programmer or dedicated repeater. The crypto key is retrieved from the source of the crypto key based on the form of the key and the type of device maintaining the crypto key. For instance, if the crypto key is stored in the IMD, the programmer retrieves the crypto key through inductive telemetry. If the crypto key is maintained in a secure database, the programmer obtains the crypto key through a secure connection to a secure server servicing the secure database. If the crypto key is provided on a physical token, the programmer includes the means for accessing the crypto key from the physical token, such as through optical, magnetic, or serial communication interfaces. Following successful authentication, the external source and the implantable medical device transact a data exchange session by transitioning to long range telemetry.

On page 8, lines 20-27, please replace the existing paragraph with the following substitute paragraph:

In a further embodiment, the IMD 103 includes a telemetry interlock that limits communication between the IMD 103 and an external device.

Patient/clinician authentication is secured through release of the telemetry interlock, which can be used in conjunction with secure crypto key 122 retrieval. The telemetry interlock is released when the external device transmits an ENABLE command to the IMD 103 via short range telemetry, such as described in commonly-assigned U.S. Patent ~~application Serial No. 10/601,763, filed June 23, 2003, pending,~~ No. 7,155,290 to Von Arx, et al., issued December 26, 2006, the disclosure of which is incorporated by reference.

On page 11, lines 7-21, please replace the existing paragraph with the following substitute paragraph:

Allows the IMD 103 and the programmer 123, repeater 124 or other wireless computing device 125 to check the integrity of the sensitive information received over an RF or other long range wireless link. Data integrity checking ensures that the only commands acted upon are those commands that have not been altered, either maliciously or accidentally. In a further embodiment, the IMD 103 verifies the integrity of messages received from a programmer 123, repeater 124 or other wireless computing device 125 and, alternatively, a programmer 123, repeater 124 or other wireless computing device 125 verifies the integrity of messages received from the IMD 103, such as described in commonly-assigned U.S. Patent ~~application Serial No. _____, entitled "Cryptographic Authentication for Telemetry With An Implantable Medical Device," Attorney Docket No. 0279.718US1, filed March 15, 2004, pending,~~ No. 7,228,182, to Healy et al., issued June 5, 2007, the disclosure of which is incorporated by reference.

On page 11, line 23 to page 12, line 6, please replace the existing paragraph with the following substitute paragraph:

Allows the IMD 103 and the programmer 123, repeater 124 or other wireless computing device 125 to encrypt and decrypt sensitive information, including any PHI, transmitted or received over an RF or other long range wireless link. Encryption allows the sensitive information to be securely

transmitted over an RF or other long range wireless link in compliance with applicable patient health information privacy laws and regulations. In a further embodiment, the programmer 123, repeater 124 or other wireless computing device 125 preencrypts sensitive information, including any PHI, which can be stored on an IMD as static data for retrieval by health care providers and for use by the IMD, such as described in commonly-assigned U.S. Patent application ~~Serial No. _____~~ Serial No. 10/801,150, entitled "System And Method For Providing Secure Exchange Of Sensitive Information With An Implantable Medical Device," ~~Attorney Docket No. 020.0329.US.UTL,~~ filed March 15, 2004, pending, the disclosure of which is incorporated by reference.

On page 12, lines 7-15, please replace the existing paragraph with the following substitute paragraph:

In one embodiment, individual commands and patient data integrity are authenticated using a standard authentication protocol, such as the Keyed-Hashed Message Authentication protocol (HMAC), and sensitive information is encrypted using a standard encryption protocol, such as the Advanced Encryption Standard protocol (AES). Other authentication and encryption techniques and protocols, as well as other functions relating to the use of the crypto key 122 are possible, including the authentication and encryption techniques and protocols described in commonly-assigned U.S. Patent ~~application Serial No. 10/601,763, filed June 23, 2003, pending,~~ No. 7,155,290, to Von Arx et al., issued December 26, 2006, the disclosure of which is incorporated by reference.